EXHIBIT 22

Email attachment excerpted and formatted for legibility

From: Pierce, Kellie [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0150EF14C7A24CB1A0E08EC9FCB06424-PIERCE, KEL]
Sent: 6/28/2019 8:37:58 PM
To: Fu, Ikong [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f7c378044ca141209da12d5a5874cff4-Fu, Ikong]; Fujii, Ross [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f2007a77afcc470289c878f02563304e-Fujii, Ross]
CC: Hansen, Jim [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d23033ce6fe14dea908e533ef92fbca3-Hansen, Jim]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]; Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject: FedRAMP - Security & Compliance Preliminary Review
Attachments: FedRAMP_Security_Controls_Baseline as of 06282019.xlsx

Good afternoon,
I've performed a preliminary review of the 325 FedRAMP Moderate controls; my takeaway is that 94% (304) of the controls will require a moderate to significant level of effort to implement.
Also, I would like to share that the work will be required from these groups within SolarWinds: Product Management, Engineering, SRE/DevOps, Facilities and DOIT.

High level based on Green/Yellow/Red:

Program/Practice in place	21	6%
Program/Practice *may* be in place but requires detailed review	106	33%
No program/practice in place	198	61%
TOTALS	**325**	**100%**

Breakdown by Control type and Green/Yellow/Red:

		Program/Practice in place	Program/Practice *may* be in place but requires detailed review	No program/practice in place	
CONTROLS					**Total**
AC	ACCESS CONTROL	2	18	23	**43**
AT	AWARENESS AND TRAINING	0	5	0	**5**
AU	AUDIT AND ACCOUNTABILITY	0	1	18	**19**
CA	SECURITY ASSESSMENT AND AUTHORIZATION	2	3	10	**15**
CM	CONFIGURATION MANAGEMENT	1	7	18	**26**
CP	CONTINGENCY PLANNING	1	19	4	**24**
IA	IDENTIFICATION AND AUTHENTICATION	0	7	20	**27**
IR	INCIDENT RESPONSE	13	3	2	**18**
MA	MAINTENANCE	0	1	10	**11**
MP	MEDIA PROTECTION	0	0	10	**10**

PE	PHYSICAL AND ENVIRONMENTAL PROTECTION	0	14	6	**20**
PL	PLANNING	0	4	2	**6**
PS	PERSONNEL SECURITY	0	0	9	**9**
RA	RISK ASSESSMENT	0	6	4	**10**
SA	SYSTEM AND SERVICES ACQUISITION	2	8	12	**22**
SC	SYSTEM AND COMMUNICATIONS PROTECTION	0	3	29	**32**
SI	SYSTEM AND INFORMATION INTEGRITY	0	7	21	**28**
	TOTAL	**21**	**106**	**198**	**325**

Please let me know if I can provide any detailed information.
Thank you,
Kellie

solarwinds
Kellie Pierce | Security & Compliance Sr. Program Manager | **SolarWinds**
Office: 512.498.6248

DOCUMENT PRODUCED IN NATIVE FORMAT

	A	B	C	D	E	F	J	S
1			NIST 800-53 Security Controls Catalog Revision 4			FedRAMP Moderate Baseline		
2	Count	SORT ID	Family	ID	Control Name	NIST Control Description (From NIST SP 800-53r4 1/23/15)	Process or Product or People?	Kellie's Comments/Notes
3	1	AC-01	ACCESS CONTROL	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency]. Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9. Control Enhancements: None. Re[illegible]	Process	KP 6/27: We have an access control policy for the organization. It would need to be updated with any specific gaps from FedRAMP and/or other certification requirments.
4	2	AC-02	ACCESS CONTROL	AC-2	ACCOUNT MANAGEMENT	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. Supplemental Guidance: Information system account types include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network	Process	KP 6/27: We do identify IT systems that are mission/bs critical, however access/role management is not strickly enforced except for SOX assets (org has 857 assets, 17 are SOX)
5	3	AC-02 (01)	ACCESS CONTROL	AC-2 (1)	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	The organization employs automated mechanisms to support the management of information system accounts. Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.	Process	KP 6/27: There is an effort by IT to automate account mgmt with Azure AD. This work is currently planned to complete 2020
6	4	AC-02 (02)	ACCESS CONTROL	AC-2 (2)	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.	Product	KP 6/27: Like with AC-2(3), this is not consistant across any IT systems. The Azure AD project will help but will take time to run across the 857 systems (124 business / mission critical)
7	5	AC-02 (03)	ACCESS CONTROL	AC-2 (3)	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	Product	KP 6/27: Agree with PM, this is not enabled across the products OR 3rd party systems used by the products
8	6	AC-02 (04)	ACCESS CONTROL	AC-2 (4)	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Related controls: AU-2, AU-12.	Product	KP 6/27: Agree with PM, but some logging has been or will be enabled for SOX impacted systems (Loggly, Papertrail)

	A	B	C	D	E	F	J	S
9	7	**AC-02 (05)**	ACCESS CONTROL	**AC-2 (5)**	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Supplemental Guidance: Related control: SC-23.	**Product**	KP 6/27: We have an access control policy for the organization. It would need to be updated with any specific gaps from FedRAMP and/or other certification requirments.
10	8	**AC-02 (07)**	ACCESS CONTROL	**AC-2 (7)**	ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES	The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example,	**Product**	KP 6/27: We have an access control policy for the organization. It would need to be updated with any specific gaps from FedRAMP and/or other certification requirments.
11	9	**AC-02 (09)**	ACCESS CONTROL	**AC-2 (9)**	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS	The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].	**Process**	KP 6/27: We have an access control policy for the organization. It would need to be updated with any specific gaps from FedRAMP and/or other certification requirments.
12	10	**AC-02 (10)**	ACCESS CONTROL	**AC-2 (10)**	ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION	The information system terminates shared/group account credentials when members leave the group.	**Product**	KP 6/27: This is connected to access management. currently systems are not integrated with AD, thereby termination of groups and/or permissions are manaual for many system.
13	11	**AC-02 (12)**	ACCESS CONTROL	**AC-2 (12)**	ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE	The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.	**Product**	KP 6/27: GAP. Currently there is no program for this across SWI
14	12	**AC-03**	ACCESS CONTROL	**AC-3**	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3. References: None.	**Product**	KP 6/27: This will require additional investigation, as I believe we would need to determine not only what happens in the product but the 3rd party systems used by the product.
15	13	**AC-04**	ACCESS CONTROL	**AC-4**	INFORMATION FLOW ENFORCEMENT	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regarding mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message- filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18. References: None.	**Product**	KP 6/27: Agree with PM. This is a gap
16	14	AC-04 (21)	ACCESS CONTROL	AC-4 (21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION	The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization- defined required separations by types of information]. Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.	Product	KP 6/27: No comment
17	15	**AC-05**	ACCESS CONTROL	**AC-5**	SEPARATION OF DUTIES	The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2. Control Enhancements: None. References: None.	**Process**	KP 6/27: This is a product question as well - we we have seen significant struggles with this requirement under SOX . For the SOX systems, we have seperation of duties in some cases, if not we have a mitigating control. Not all of the cloud products are in scope of SOX.

	A	B	C	D	E	F	J	S
18	16	**AC-06**	ACCESS CONTROL	**AC-6**	LEAST PRIVILEGE	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2. References: None.	**Process**	KP 6/27: This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.
19	17	**AC-06 (01)**	ACCESS CONTROL	**AC-6 (1)**	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]. Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.	**Process**	KP 6/27: We have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products
20	18	**AC-06 (02)**	ACCESS CONTROL	**AC-6 (2)**	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non- privileged accounts or roles, when accessing nonsecurity functions. Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.	**Process**	KP 6/27: This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.
21	19	**AC-06 (05)**	ACCESS CONTROL	**AC-6 (5)**	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.	**Process**	KP 6/27: We have no explicit restriction policy, nor is this documented that I am aware of for the company or individual products
22	20	**AC-06 (09)**	ACCESS CONTROL	**AC-6 (9)**	LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS	The information system audits the execution of privileged functions. Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.	**Product**	KP 6/27: Agree with PM. There is currently no audit
23	21	**AC-06 (10)**	ACCESS CONTROL	**AC-6 (10)**	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.	**Product**	KP 6/27: This has not been tested/audited, nor is a policy documented.
24	22	**AC-07**	ACCESS CONTROL	**AC-7**	UNSUCCESSFUL LOGON ATTEMPTS	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5. References: None.	**Product**	KP 6/27: Some IT systems have this enabled but it is not consistant across the products
25	23	**AC-08**	ACCESS CONTROL	**AC-8**	SYSTEM USE NOTIFICATION	The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and	**Product**	KP 6/27: Agree with PM, this is a gap
26	24	**AC-10**	ACCESS CONTROL	**AC-10**	CONCURRENT SESSION CONTROL	The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. Control Enhancements: None. References: None.	**Product**	KP 6/27: Agree with PM, this is a gap

	A	B	C	D	E	F	J	S
27	25	**AC-11**	ACCESS CONTROL	**AC-11**	SESSION LOCK	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related	**Product**	KP 6/27: Agree with PM, this is a gap
28	26	**AC-11 (01)**	ACCESS CONTROL	**AC-11 (1)**	SESSION LOCK | PATTERN-HIDING DISPLAYS	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information. References: OMB Memorandum 06-16.	**Product**	KP 6/27: Agree with PM, this is a gap
29	27	**AC-12**	ACCESS CONTROL	**AC-12**	SESSION TERMINATION	The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect]. Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.	**Product**	KP 6/27: Agree with PM, this is a gap
30	28	**AC-14**	ACCESS CONTROL	**AC-14**	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2. Control Enhancements: None. (1) PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES [Withdrawn: Incorporated into AC-14]. References: None.	**Process**	KP 6/27: Assets and systems are identified as mission/bs critical. We have a Major Incident and Security Incident plans documented as to how we handle mission/bs critical assets
31	29	**AC-17**	ACCESS CONTROL	**AC-17**	REMOTE ACCESS	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections. Supplemental Guidance: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4. References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.	**Process**	KP 6/27: The organzation has rules around accessing systems remotly. This may not apply to the AppMan products but would apply to supporting IT systems/network
32	30	**AC-17 (01)**	ACCESS CONTROL	**AC-17 (1)**	REMOTE ACCESS | AUTOMATED MONITORING / CONTROL	The information system monitors and controls remote access methods. Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.	**Product**	KP 6/27: There are security monitoring tools and a practice to review issues. FedRAMP assets would need to be specifically reviewed.
33	31	**AC-17 (02)**	ACCESS CONTROL	**AC-17 (2)**	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.	**Product**	KP 6/27: Please confirm. Loggly does not have encryption in place nor does AO per the SOC2 work. Papertrail and Pingdom are unknown
34	32	**AC-17 (03)**	ACCESS CONTROL	**AC-17 (3)**	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.	**Product**	KP 6/27: IT does manage remote access but "all" would need to be audited to confirm.
35	33	**AC-17 (04)**	ACCESS CONTROL	**AC-17 (4)**	REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. Supplemental Guidance: Related control: AC-6.	**Process**	KP 6/27: I do not believe this is documented.
36	34	**AC-17 (09)**	ACCESS CONTROL	**AC-17 (9)**	REMOTE ACCESS | DISCONNECT / DISABLE ACCESS	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.	**Product**	KP 6/27: Agree with PM- this is not in place for any products and may be somewhat in place for IT managed assets

	A	B	C	D	E	F	J	S
37	35	**AC-18**	ACCESS CONTROL	**AC-18**	WIRELESS ACCESS	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections. Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.	**Process**	KP 6/27: We have some wireless requirements in the Access/Security guidelines howevver they need to be reviewed against the FedRAMP requirements
38	36	**AC-18 (01)**	ACCESS CONTROL	**AC-18 (1)**	WIRELESS ACCESS | AUTHENTICATIO N AND ENCRYPTION	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. Supplemental Guidance: Related controls: SC-8, SC-13.	**Product**	KP 6/27: We have some wireless requirements in the Access/Security guidelines howevver they need to be reviewed against the FedRAMP requirements
39	37	**AC-19**	ACCESS CONTROL	**AC-19**	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non- removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.	**Process**	KP 6/27: The company does not have a policy on non-network devices connecting to the network.
40	38	**AC-19 (05)**	ACCESS CONTROL	**AC-19 (5)**	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED	The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.	**Process**	KP 6/27: The company does not have an access control for mobile devices
41	39	**AC-20**	ACCESS CONTROL	**AC-20**	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal	**Process**	KP 6/27: Procurement has a process in place for T& C and Data Processing Addendum
42	40	**AC-20 (01)**	ACCESS CONTROL	**AC-20 (1)**	USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.	**Process**	KP 6/27: The company has some Data Loss Prevention montiring however no hard blocks on information. This is a will take signifincant change.
43	41	**AC-20 (02)**	ACCESS CONTROL	**AC-20 (2)**	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE	The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems. Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	**Process**	KP 6/27: There is no policy around portable storage devices
44	42	**AC-21**	ACCESS CONTROL	**AC-21**	INFORMATION SHARING	The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3. References: None.	**Process**	6/27 KP: authorized v.s unauthorized users has not been defined and policies are not fully comprehensive to meet this control
45	43	**AC-22**	ACCESS CONTROL	**AC-22**	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.	**Process**	6/27 KP: We have a communication process in place with approval gates (marketing/legal) however I am unsure if this is clearly documented.
46	44	**AT-01**	AWARENESS AND TRAINING	**AT-1**	SECURITY AWARENESS AND TRAINING POLICY ANDPROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place